

Installationsleitfaden

EVault Agent für Windows



Inhalt

1.	Technische Informationen	- 1 -
1.1.	Firewall – Ports	- 1 -
1.2.	Hinweis zur Dokumentation.....	- 1 -
1.3.	Hintergrundwissen	- 1 -
1.4.	Ihr Zugang.....	- 2 -
1.5.	Support.....	- 2 -
2.	Erste Schritte im Webinterface.....	- 3 -
2.1.	Anmelden am Web Frontend	- 3 -
2.2.	Anlegen von Benutzern.....	- 3 -
3.	Installation und Konfiguration des Agents	- 6 -
3.1.	Installation des EVault Agents	- 6 -
3.2.	Konfiguration des Agents	- 9 -
3.3.	Hinzufügen eines Vault Profils	- 9 -
3.4.	Anlegen von Aufbewahrungstypen	- 11 -
3.5.	Anlegen von Benachrichtigungen.....	- 13 -
4.	Datensicherung	- 14 -
4.1.	Einrichtung einer Datensicherung	- 14 -
4.2.	Einrichtung einer BMR-Sicherung.....	- 18 -
4.3.	Einrichtung einer Sicherung eines UNC-Dateien.....	- 22 -
4.4.	Änderung von bestehenden Sicherungen.....	- 26 -
5.	Restore von Datensicherungen	- 27 -
5.1.	Restore einer filebasierenden Datensicherung	- 27 -
5.2.	Restore einer BMR-Sicherung	- 30 -

1. Technische Informationen

1.1. Firewall – Ports

Die folgenden Ports sind „**ausgehend**“ an Ihrer Firewall freizuschalten.

Port	Verwendung	Protokoll	Ziel
8086	Anbindung des Agents an das Webportal.	TCP	89.251.128.130
8087	Anbindung des Agents an das Webportal.	TCP	89.251.128.140
2546	Datenverbindung vom Agent zum Sicherungsserver.	TCP	89.251.128.0/24 89.251.131.80/28
2547	Datenverbindung vom Satelliten zum Sicherungsserver (wird nur beim Einsatz eines Satelliten benötigt).	TCP	89.251.128.0/24 89.251.131.80/28
12547	Datenverbindung vom Satelliten zum Sicherungsserver (wird nur beim Einsatz eines Satelliten benötigt).	TCP	89.251.128.0/24 89.251.131.80/28
25	Mailbenachrichtigung durch den Agent.	TCP	In der Mailkonfiguration des Agents angegebenen Mailserver.

1.2. Hinweis zur Dokumentation

Bitte lesen Sie diese Dokumentation sehr sorgfältig durch. Bei einigen Konfigurationspunkten sind Arbeiten vorab zu erledigen.

1.3. Hintergrundwissen

Bei der Sicherung mit dem Produkt EVault handelt es sich um eine Online-Backup. Die Sicherung Ihrer Computer sowie die Konfiguration der Sicherungsjobs erfolgt „**online**“. Eine Internetverbindung ist daher zwingend notwendig.

Je nach Sicherungsgröße und Bandbreite Ihrer Internetverbindung empfiehlt sich der Einsatz eines sogenannten „**Backup-Satelliten**“. Hierbei handelt es sich um einen weiteren Sicherungsserver, der am Standort Ihrer zu sichernden Server aufgestellt wird. Die Sicherung erfolgt dann in zwei Schritten: Die eigentliche Sicherung erfolgt standortintern auf den Satelliten. Anschließend werden die auf den Satelliten gesicherten Daten auf die Sicherungsserver im Rechenzentrum der microPLAN GmbH repliziert.

Zusätzlich gibt es die Möglichkeit das Initialbackup bei größeren Sicherungen mittels einer „**Starterbox**“ ins Rechenzentrum zu liefern. Hierbei handelt es sich um einen Sicherungsserver, der für den Zeitraum der Erstsicherung am Standort Ihrer Server aufgestellt wird. Nach dem Abschluss der Erstsicherung wird diese Starterbox an das Rechenzentrum geliefert und die Erstsicherung hierhin importiert. Anschließend kann die normale Sicherung über die Internetverbindung in Betrieb genommen werden.

In Abhängigkeit der zu sichernden Datenmenge und der Bandbreite der verwendeten Internetverbindung kann das Initialbackup durchaus mehrere Tage dauern.

1.4. Ihr Zugang

Nach der Bestellung eines Demozugangs bzw. der Beauftragung einer Onlinesicherung, erhalten Sie von uns eine E-Mail mit Zugangsdaten. Mit diesen Zugangsdaten erhalten Sie Zugriff auf das Web Frontend der Onlinesicherung. Loggen Sie sich unter <https://backup.rz-24.de/> mit Ihren Zugangsdaten ein.

1.5. Support

Sollte es weitergehende Fragen oder Probleme geben, stehen wir Ihnen selbstverständlich gerne zur Verfügung. Wenden Sie sich einfach an unseren Support:

E-Mail: technik@microPLAN.de

Wir sind telefonisch für Sie erreichbar:

Mo-Fr 07:30 Uhr – 17:30 Uhr

Tel.: 02572 / 93 65 400

2. Erste Schritte im Webinterface

Hier soll Ihnen erläutert werden, wie Sie Schritt für Schritt zu Ihrer Datensicherung kommen.

2.1. Anmelden am Web Frontend

Das Web Frontend ist das zentrale Tool zur Verwaltung Ihrer Sicherung. Die komplette Sicherung inklusive Benachrichtigungen, Protokolle und Co. wird hiermit verwaltet.

URL:

<https://backup.rz-24.de/>

Benutzername:

Ihr Benutzer

Kennwort:

Ihr Kennwort



de

RZ-24 ONLINE BACKUP

Benutzername

Kennwort

Anmelden

☐ Anmeldeinformationen speichern?

☐ Bei der alten Web CentralControl-Oberfläche anmelden

Hinweis:

Bitte verwenden Sie nicht die alte „**Web CentralControl-Oberfläche**“. Dieses Portal bietet nur einen eingeschränkten Funktionsumfang.

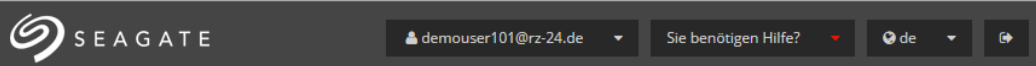
2.2. Anlegen von Benutzern

Wir empfehlen einen gesonderten Benutzer anzulegen, mit dem die Sicherungsagents bei der Installation am Webportal registriert werden. Dies hat den Hintergrund, dass Sie, wenn Sie die Agents mit Ihrem „**normalen**“ Benutzer registrieren, diese neu registrieren müssen, wenn Sie das Kennwort Ihres Benutzers ändern.

Für die Registrierung eines neuen Agents reicht es, wenn der verwendete Benutzer der Rolle „Benutzer“ angehört.

Um einen Benutzer anzulegen, gehen Sie bitte wie folgt vor.

1. Klicken Sie in der Navigation „**oben**“ auf Ihren Benutzernamen.



2. Im erscheinenden Dropdown Menü haben Sie nun die Möglichkeit, den „**Benutzermanager**“ aufzurufen.

Kontext Menü im Detail

Folgende Optionen werden angeboten:

1. Mein Kennwort ändern
2. Meine Einstellungen
3. Meine Site-Einstellungen
4. Benutzermanager
5. Abmelden

Zum Anlegen eines neuen Benutzers verwenden Sie den Punkt 4 (Benutzermanager).

demouser101@rz-24.de ▼

Mein Kennwort ändern

Meine Einstellungen

Meine Site-Einstellungen

Benutzermanager

Abmelden

3. Nachdem Sie den Benutzermanager aufgerufen haben, sehen Sie im oberen Teil der Webseiten den Menüpunkt „**Neuen Benutzer erstellen**“. Wählen Sie bitte diese Option um einen neuen Benutzer zu erstellen.

Kontext Menü im Detail

Folgende Optionen werden angeboten:

1. „+ **Neuen Benutzer erstellen**“

Dieser Menüpunkt ruft die Option „Seite“ auf, mit deren Hilfe Sie einen neuen Benutzer für die Installation der Agents erstellen zu können.

SEAGATE

Dashboard Computer

+ Neuen Benutzer erstellen

4. Zum Anlegen eines Benutzers müssen alle Felder ausgefüllt sein.
- Füllen Sie die Felder aus.
 - Beachten Sie die Kennwort-Hinweise.
 - Sobald alle Felder ausgefüllt sind, können Sie unten rechts auf „**Erstellen**“ klicken.

Allgemeine Informationen

E-Mail-Adresse (Benutzername):

Kundenname@kd.microplan.de

Vorname:

Kunden

Nachname:

Name

Rolle:

Benutzer

Kennwort

Kennwort:

Kennwort bestätigen:

☐ Benutzer muss das Kennwort ändern:

Benutzer-Rollen

Administrator:

Ein Benutzer vom Typ „Administrator“ darf Agents registrieren und konfigurieren, Jobs anlegen und ausführen und Benutzer anlegen.

Benutzer:

Ein Benutzer der Rolle „Benutzer“ darf Agents registrieren, von ihm registrierte oder zugewiesene Agents konfigurieren sowie bei diesen Agents Jobs anlegen und ausführen.

Nur ausführen:

Ein Benutzer der Rolle „Nur ausführen“ darf bereits angelegte Jobs und die jeweiligen zugewiesenen Agents ausführen und Restore-Jobs auf diesen Server konfigurieren und starten.

Nur lesen:

Ein Benutzer der Rolle „Nur lesen“ darf nur den Status der von ihm zugewiesenen Agents und Jobs sehen.

3. Installation und Konfiguration des Agents

3.1. Installation des EVault Agents

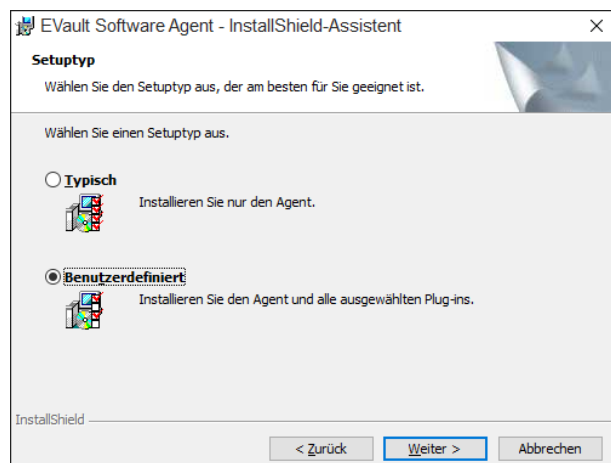
Damit überhaupt gesichert werden kann, muss der zu „**sichernde Computer**“ mit einem Agent ausgestattet werden.

Hier wird Ihnen beschrieben wie die Installation des EVault Agents durchgeführt werden muss. Diese Anleitung behandelt die Installation des einfachen Windows Agents zur Sicherung von Dateien oder einer BMR-Sicherung. Für die Sicherung von Datenbanken oder eines Exchanges sind zusätzliche Plugins nötig. Die Anleitungen und die benötigten Installationspakete finden Sie im Downloadbereich unserer Website.

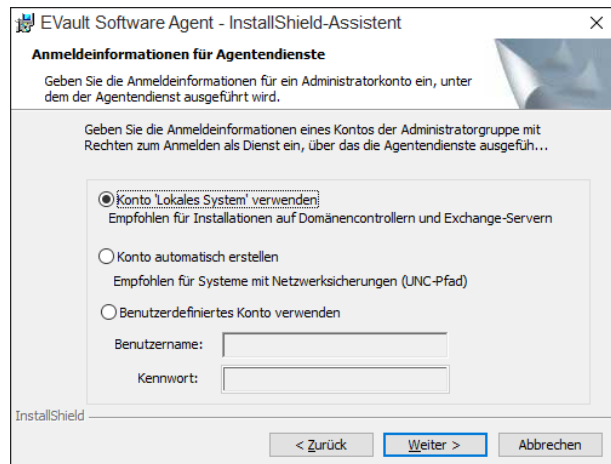
Bei der Auswahl des Installationspaketes ist zu beachten, dass es separate Installationspakete für 32- und 64-Bit gibt. Sie müssen also das entsprechende Installationspaket herunterladen und ausführen. Anschließend wählen Sie die gewünschte Sprache der Installation aus (die Anleitung basiert auf der deutschen Installation) und bestätigen die folgenden Informations- und Lizenzbedingungsseiten.

Hinweis: Beim Start der Installation wird geprüft, ob noch ein Neustart von anderen Installationen aussteht. Sollte dies der Fall sein, bricht die Sicherung ab und lässt sich erst nach dem Neustart des Systems fortführen.

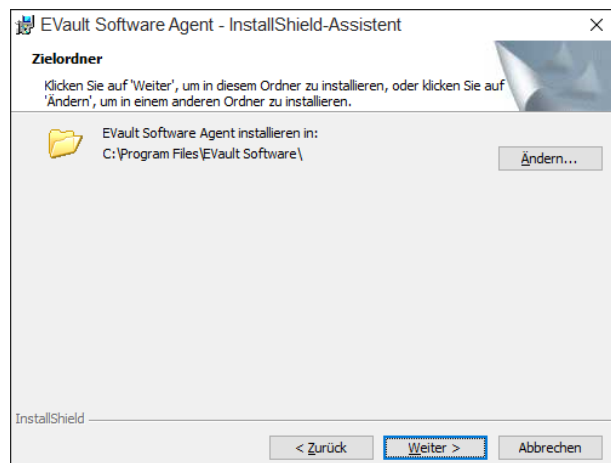
Um Einfluss darauf zu haben, welche Plugins installiert werden, empfehlen wir die „**benutzerdefinierte**“ Installation auszuwählen.



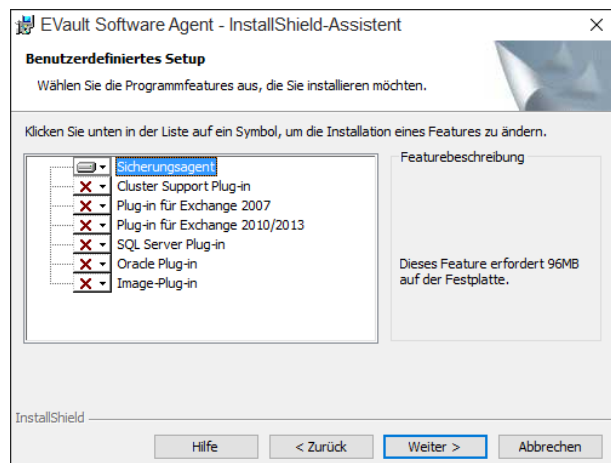
Als nächstes wird abgefragt, unter welchem Konto der Sicherungsagent ausgeführt werden soll. Das Konto „**lokales System**“ ist vollkommen ausreichend.



Im nächsten Schritt muss der Installationspfad gewählt werden.

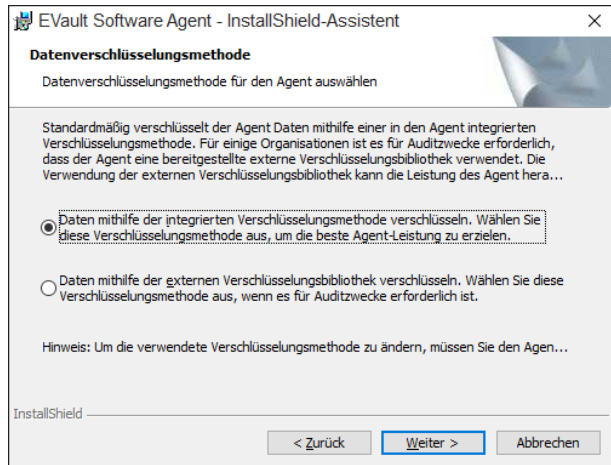


Als nächstes muss festgelegt werden was installiert werden soll. Für die Datei und BMR-Sicherung reicht der „**Sicherungsagent**“ aus.



Nun kann noch ausgewählt werden, welche Verschlüsselungsmethode genutzt werden soll. Es empfiehlt sich die integrierte AES-Verschlüsselung zu verwenden, da der Agent für die Nutzung dieser Verschlüsselung optimiert ist.

Hinweis: Möchten Sie eine andere Verschlüsselung verwenden, muss diese vor der Installation des Agents installiert werden.



Abschließend muss der Agent noch am Webportal registriert werden.

Netzwerkadresse:

- backup.rz-24.de

Port:

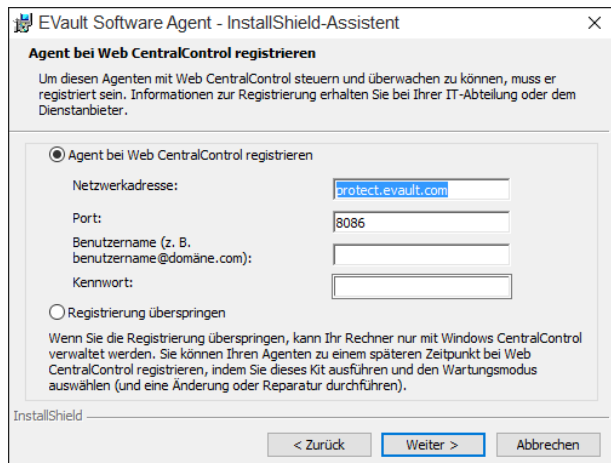
- 8086

Benutzername:

- Der Ihnen mitgeteilte Benutzername bzw. der von Ihnen angelegte Benutzer aus dem Webportal.

Kennwort:

- Das Ihnen mitgeteilte Kennwort bzw. im Webportal angelegte Kennwort.



Hinweis / Empfehlung:

- Legen Sie den entsprechenden Benutzer im Webportal an.
- Wird die Registrierung übersprungen, sind die weiteren Schritte nicht möglich.

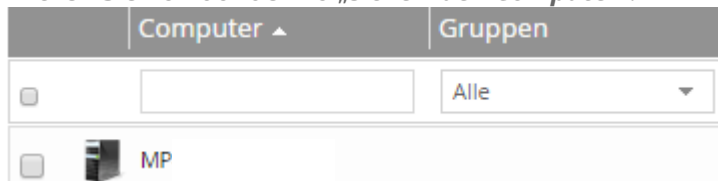
3.2. Konfiguration des Agents

Nach dem Abschluss der Installation erscheint der Agent automatisch im Web Frontend und kann nun hierüber konfiguriert werden.

1. Klicken Sie in der Navigation auf den Menüpunkt „**Computer**“.

Dashboard Computer Überwachung Berichte Richtlinien

2. Klicken Sie nun auf den zu „**sichernden Computer**“.



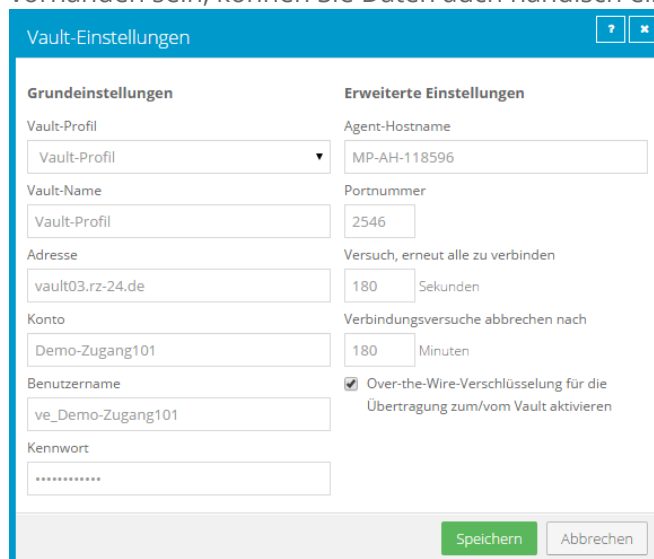
3. Wählen Sie in der folgenden Ansicht entsprechenden den Menüpunkt „**manuell konfigurieren**“.

Manuell konfigurieren durch Bereitstellen von bestimmten Agent- und Vault-Einstellungen.

3.3. Hinzufügen eines Vault Profils

Als erstes muss dem Agent ein Vault Profil zugewiesen werden. Das Vault Profil beschreibt das Sicherungsziel.

1. Klicken Sie dazu bitte auf den Button „**+Vault hinzufügen**“ im rechten Teil der Ansicht.
2. Hier wird Ihnen im Dropdown-Menü das entsprechende Profil zur Auswahl angeboten. Sollten Sie einen Satelliten einsetzen, muss ggf. die Adresse der URL auf die IP-Adresse des Satelliten umgestellt werden. Sollte das gewünschte Profil nicht vorhanden sein, können Sie Daten auch händisch eingeben.



Vault Einstellungen im Detail

Diese Ansicht erläutert die entsprechenden Punkte, die Sie im obigen Schaubild sehen können.

Vault Profile	Auswahl der hinterlegten Profile.
Vault Name	Name des Vault (kann frei vergeben werden).
Adresse	Adresse des Sicherungsziels.
Konto	Der Name Ihres Sicherungskontos (wird von der microPLAN GmbH vergeben).
Benutzername	Der Anmeldenname Ihres Sicherungskontos (wird von der microPLAN GmbH vergeben).
Kennwort	Das Kennwort Ihres Sicherungskontos (wird von der microPLAN GmbH vergeben).
Agents Hostname	Definiert den Namen unter dem der Agent in den Reports angezeigt wird. Dieser Name kann nachträglich nicht mehr geändert werden.
Portnummer	2546 - Der Port für die Datenverbindung.
Versuch, erneut alle zu verbinden	Definiert die Zeit zwischen zwei Verbindungsversuchen zum Sicherungsserver, wenn der Verbindungsaufbau fehlschlägt.
Verbindungsversuche Abbrechen nach	Definiert den Zeitraum, nach dem die Verbindungsversuche abgebrochen werden.

Hinweis

Auch hier muss gespeichert werden!

3.4. Anlegen von Aufbewahrungstypen

Mit Hilfe von „**Aufbewahrungstypen**“ wird festgelegt, wie lange eine Sicherung auf dem Vault gespeichert werden.

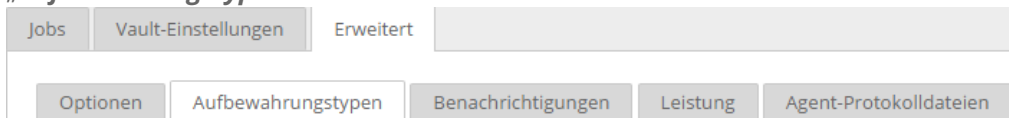
Standardmäßig sind 3 Aufbewahrungstypen vorkonfiguriert:

Daily : es werden bis zu 7 Sicherungen 7 Tage aufbewahrt.
Weekly : es werden bis zu 5 Sicherungen 31 Tage aufbewahrt.
Monthly : es werden bis zu 12 Sicherungen 365 Tage aufbewahrt.

Darüber hinaus können Sie beliebig viele individuelle Aufbewahrungstypen erstellen.

Um einen individuellen Aufbewahrungsplan zu erstellen, gehen Sie bitte wie folgt vor:

1. Wählen Sie nun den Menüpunkt „**Erweitert**“ und im unteren Teil den Punkt „**Aufbewahrungstypen**“.



2. Ihnen wird nun eine Auflistung mit allen vorhandenen Aufbewahrungstypen angezeigt.

Aufbewahrungsname	Onlinespeicherung (Tage)	Onlinekopien	Archivierungsdauer (Tage)	
Daily	7	7	---	 
Monthly	365	12	---	 
Weekly	31	5	---	 

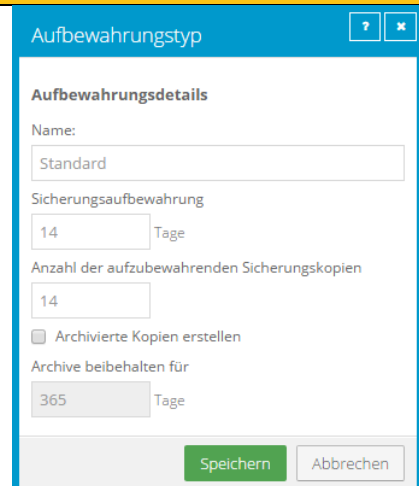
3. Sie haben hier nun die Möglichkeit eigene „**Aufbewahrungstypen**“ anzulegen. Klicken Sie dazu im oberen Teil auf den Button „**+Aufbewahrungstypen erstellen**“. Es öffnet sich nun ein Fenster, in dem Sie einen „**Aufbewahrungstypen**“ erstellen können.

Aufbewahrungstypen erstellen im Detail

Hier haben Sie die Möglichkeit einen neuen Aufbewahrungstypen zu erstellen.

1. Vergeben Sie einen beliebigen Namen.

2. Definieren Sie, wie lange eine Sicherung dieses Aufbewahrungstyps gespeichert werden soll.



Aufbewahrungstyp

Aufbewahrungsdetails

Name:

Sicherungsaufbewahrung: Tage

Anzahl der aufzubewahrenden Sicherungskopien:

☐ Archivierte Kopien erstellen

Archive beibehalten für: Tage

Speichern **Abbrechen**

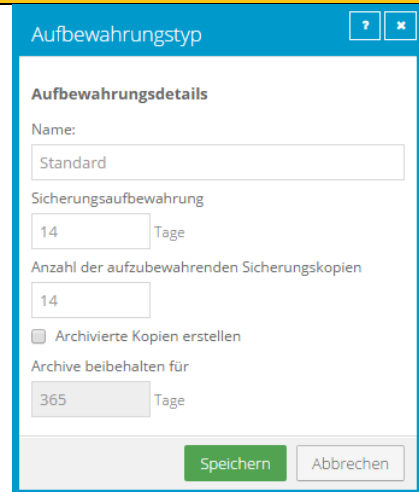
3. Legen Sie die Anzahl der Kopien fest, die gespeichert werden sollen.

4. Speichern Sie.

Beispiel:

Es soll 6 Sicherungen 6 Monate gespeichert werden.

1. Vergeben Sie einen Namen.
2. Stellen Sie die „**Sicherungsaufbewahrung**“ auf 186 Tage ein.
3. Stellen Sie die „**Anzahl der aufzubewahrenden Sicherungskopien**“ auf 6 ein.



Achtung: Beide Bedingungen müssen erfüllt sein, damit ein Safeset gelöscht wird.

Gemäß oben genannten Beispiel: Wird eine Sicherung innerhalb der 186 Tage ein 7. Mal ausgeführt, wird das älteste Safeset erst dann gelöscht, wenn es 186 Tage alt ist. Ebenso würde ein Safeset, das zwar 186 Tage alt ist, aber nur 5 Versionen aufweist, erst gelöscht, wenn die Anzahl von 6 Safesets erreicht ist.

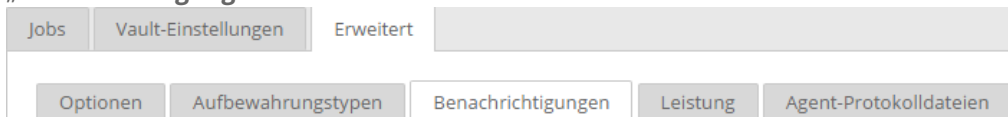
3.5. Anlegen von Benachrichtigungen

Benachrichtigungen dienen der Information. Wird diese Funktion aktiviert, versendet der Agent bei Abschluss jeder Sicherung die dieser Agent ausführt, eine Benachrichtigung.

Hinweis: Die Benachrichtigungen werden per E-Mail an einen Empfänger geschickt. Sie benötigen hierzu einen Mailserver, der vom Agent aus per SMTP erreichbar ist. Es wird kein Mailserver durch die microPLAN GmbH gestellt.

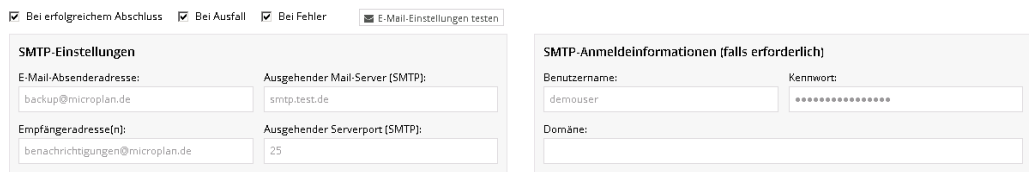
Um dem Agent eine Benachrichtigung hinzuzufügen, gehen Sie bitte wie folgt vor:

1. Wählen Sie nun den Menüpunkt „**Erweitert**“ und im unteren Teil den Punkt „**Benachrichtigungen**“



The screenshot shows the configuration window with tabs: Jobs, Vault-Einstellungen, Erweitert, and an unlabeled tab. Under the 'Erweitert' tab, there are sub-tabs: Optionen, Aufbewahrungstypen, Benachrichtigungen (selected), Leistung, and Agent-Protokolldateien.

2. Sie müssen nun eine Absenderadresse, einen erreichbaren Mail-Server sowie eine Zieladresse angeben. Zusätzlich haben Sie die Möglichkeit Authentifikationsdaten zu hinterlegen.



The screenshot shows the 'SMTP-Einstellungen' (SMTP Settings) section with the following fields:

- ☒ Bei erfolgreichem Abschluss
- ☒ Bei Ausfall
- ☒ Bei Fehler
- ☐ E-Mail-Einstellungen testen

SMTP-Einstellungen

E-Mail-Absenderadresse: backup@microplan.de	Ausgehender Mail-Server (SMTP): smtp.test.de
Empfängeradresse(n): benachrichtigungen@microplan.de	Ausgehender Serverport (SMTP): 25

SMTP-Anmeldeinformationen (falls erforderlich)

Benutzername: demouser	Kennwort: *****
Domäne:	

Folgende Optionen zur Benachrichtigung stehen Ihnen zur Verfügung:

- Bei einem erfolgreichem Abschluss: Nach erfolgreicher Sicherung
- Bei Ausfall: Wenn ein Ausführzeitpunkt verpasst wurde
- Bei Fehler: Bei fehlgeschlagenen Sicherungen

4. Datensicherung

Nun da der Agent konfiguriert ist, können die Sicherungen angelegt werden.

1. Wählen Sie nun den Menüpunkt „**Jobs**“.

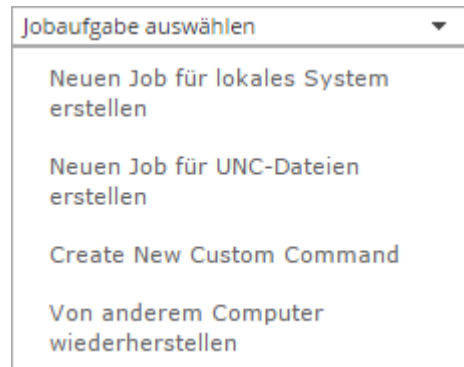


2. Nun können Sie im rechten Teil der Webseite den Menüpunkt „**Jobaufgabe auswählen**“ klicken.

Jobaufgabe im Detail

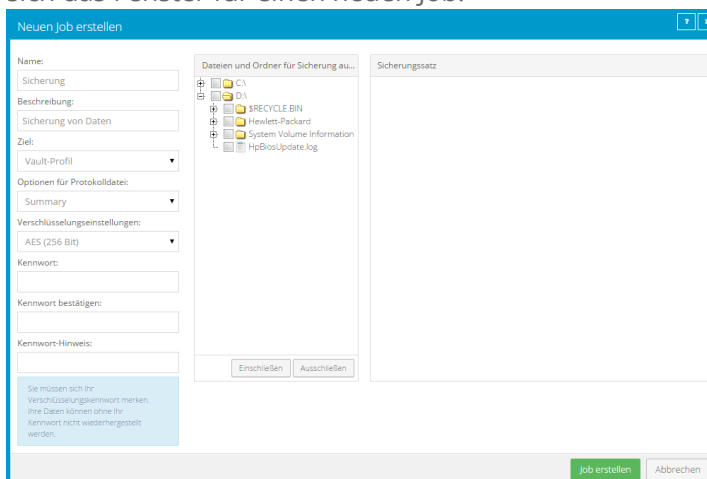
Im Dropdown-Menü haben Sie nun diverse Möglichkeiten eine Job anzulegen. Der Inhalt des Dropdown-Menüs variiert je nach installierten Plugins. Im aktuell behandelten Beispiel sind die folgenden Jobs vorhanden:

1. Neuen Job für ein lokales System erstellen
2. Neuen Job für UNC-Dateien erstellen.
3. Create New Custom Command
4. Von anderem Computer wiederherstellen



4.1. Einrichtung einer Datensicherung

1. Um eine Sicherung von lokalen Daten anzulegen, wählen Sie den Menüpunkt „**Neuen Job für ein lokales System erstellen**“.
2. Nachdem Sie „**Neuen Job für ein lokales System erstellen**“ gewählt haben, öffnet sich das Fenster für einen neuen Job.



Neuen Job erstellen im Detail

Um einen neuen Job zu erstellen, müssen in der linken Spalte folgende Einstellungen als erstes vorgenommen werden:

1. Es muss ein Name für den Sicherungsjob vergeben werden.

Name:

2. Es kann eine Beschreibung hinzugefügt werden.

Beschreibung:

3. Das Sicherungsziel muss zugewiesen werden. (Hier können nur die vorher dem Agent zugewiesenen Vault Profile ausgewählt werden.)

Ziel:

4. Hier wird die Art der Protokollierung des Jobs festgelegt. Im normalen Betrieb sollte „**Summary**“ vollkommen ausreichen.

Optionen für Protokolldatei:

5. Hier kann die Verschlüsselungsart ausgewählt werden. Standardmäßig ist „**AES**“ ausgewählt. Sollten Sie bei der Installation des Agents eine eigene Verschlüsselungsbibliothek installiert haben, steht Ihnen diese hier ebenfalls zur Verfügung. Alternativ wird auch die Möglichkeit geboten die Verschlüsselung abzuschalten. Allerdings nehmen die Sicherungsserver der microPLAN GmbH unverschlüsselte Sicherungen nicht an.

Verschlüsselungseinstellungen:

6. Abschließend wird noch das Verschlüsselungskennwort vergeben.

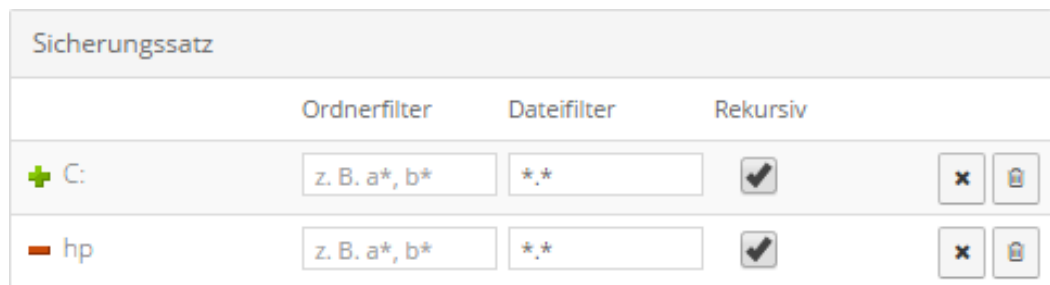
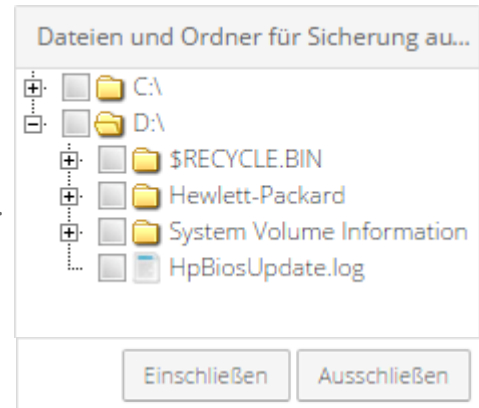
Hinweis zum Verschlüsseln:

1. Bewahren Sie das Verschlüsselungskennwort gut auf. Ohne das Verschlüsselungskennwort ist kein Zugriff auf Ihre gesicherten Daten und somit auch keine Wiederherstellung möglich.

Kennwort:**Kennwort bestätigen:****Kennwort-Hinweis:**

2. Wenn das Verschlüsselungskennwort geändert wird, wird automatisch eine neue Vollsicherung durchgeführt.

Nun können Sie in der mittleren Spalte festlegen was gesichert werden soll. Hierzu wählen Sie die zu sichernden Verzeichnisse, zum Beispiel C:\, und bestätigen die Auswahl mit „**Einschließen**“. Nun können Sie noch Unterordner von der Sicherung ausschließen. Wenn zum Beispiel der Ordner C:\HP nicht mit gesichert werden soll, wählen Sie diesen aus und bestätigen die Auswahl mit „**Ausschließen**“. Somit wird in unserem Beispiel C:\ mit allen Unterordnern, außer C:\HP und dessen Unterordner, gesichert.

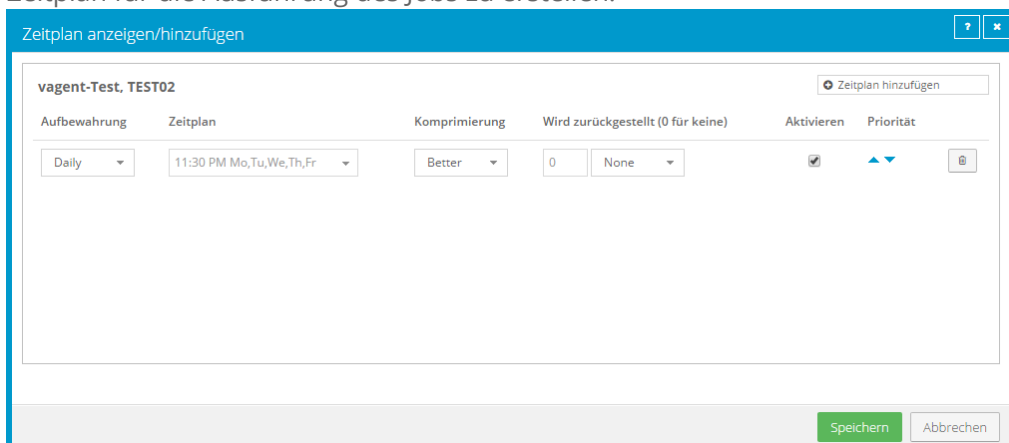


Abschließend haben Sie in der rechten Spalte noch die Möglichkeit über „**Filter**“ Ordner mit bestimmten Namen oder Namensteilen sowie bestimmte Dateien aus der Auswahl auszuschließen. Hierbei ist zu beachten, dass nur der Dateifilter rekursiv angewendet werden kann. Ein Ordnerfilter gilt immer nur für die oberste Ordnerstufe der Auswahl.

Möchten Sie jetzt zum Beispiel tmp-Dateien auf C:\ nicht mitsichern, müssten Sie in das Dateifilterfeld „***.tmp**“ eintragen.

Nachdem Sie die Auswahl der zu sichernden Daten fertiggestellt haben, speichern Sie den Job mit „Job erstellen“.

- Nachdem Sie den Job erstellt haben, haben Sie nun noch die Möglichkeit, einen Zeitplan für die Ausführung des Jobs zu erstellen.



Anlegen eines Zeitplans im Detail

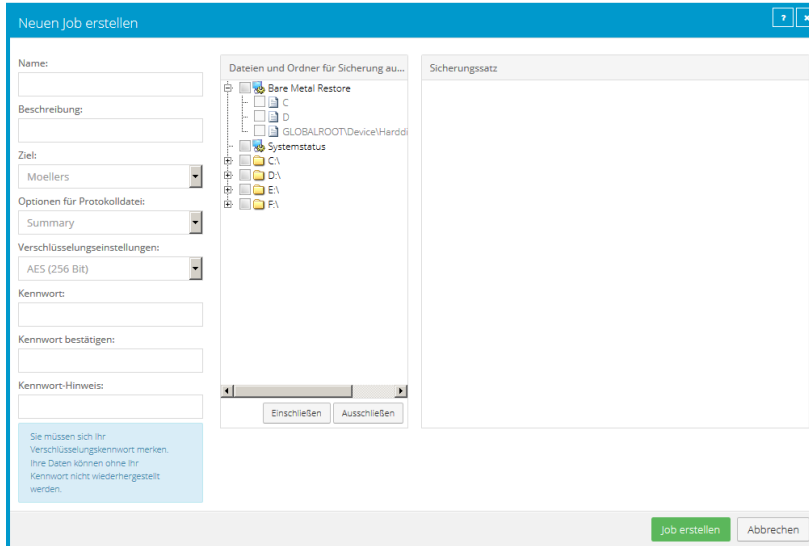
Aufbewahrung	Hier müssen Sie einen Aufbewahrungstyp auswählen, der das Aufbewahrungsmuster Ihrer Sicherung bestimmt.
Zeitplan	Hier stellen Sie ein, wann und wie spät Ihre Sicherung ausgeführt wird. Zur Auswahl stehen Tage der Woche, Tage des Monats, so wie die Möglichkeit eigene Startzeitpunkte zu definieren
Komprimierung	Achtung: Beachten Sie das US Zeitformat AM / PM. Hier kann der Grad der Komprimierung eingestellt werden. Den besten Kompromiss zwischen Rechenlast und Komprimierungsgrad bietet „ Better “.
Wird zurückgestellt	Diese Option bietet die Möglichkeit die Sicherung, nach einem bestimmten Zeitfenster, abubrechen und die noch nicht gesicherten Daten bis zur nächsten Sicherung zurückzustellen. Achtung: Da bei der nächsten Sicherung die Prüfung der Dateien auf Änderungen von vorne beginnt, kann dies dazu führen, dass wenn die Menge der geänderten Daten dauerhaft zu groß für das Sicherungszeitfenster ist, Daten am Ende der Auswahl nie gesichert werden.
Aktivieren	Diese Option aktiviert und deaktiviert den Zeitplan.
Priorität	In Zeitplänen mit mehreren einzelnen Zeitplänen können diese über die Prioritätspfeile sortiert werden. Achtung: Bei mehreren Zeitplänen wird immer der erste zutreffende verwendet.

- Vom System wird bei der Konfiguration automatisch ein Zeitplan angelegt. Weitere Zeitpläne können Sie oben rechts über den Button „**+Zeitplan Hinzufügen**“ hinzufügen. Hierbei ist zu beachten, dass der Zeitplan der am seltensten ausgeführt wird, an oberster Stelle steht.

Möchten Sie also eine Sicherung erstellen, die täglich läuft und zusätzlich eine Wochen- und Monatssicherung durchführt, müsste als oberstes die Monatssicherung aufgeführt werden, dann die Wochensicherung und als unterstes die Tagessicherung. Wenn mehrere Zeitpläne gleichzeitig zutreffen, aber die Sicherung nur einmal durchgeführt werden soll (zum Beispiel bei einer Tagessicherung, die jeden Tag läuft und einer Monatssicherung die an jedem ersten des Monats ausgeführt wird), muss der Startzeitpunkt gleich sein. Sobald alle Einstellungen getroffen wurden, beenden Sie die Konfiguration des Jobs, indem Sie auf „**Speichern**“ klicken.

4.2. Einrichtung einer BMR-Sicherung

- Um eine BMR-Sicherung anzulegen, wählen Sie der Menüpunkt „**Neuen Job für ein lokales System erstellen**“.
- Nachdem Sie „**Neuen Job für ein lokales System erstellen**“ gewählt haben, öffnet sich das Fenster für einen neuen Job.



Neuen Job erstellen im Detail

Um einen neuen Job zu erstellen, müssen in der linken Spalte folgende Einstellungen als erstes vorgenommen werden:

- Es muss ein Name für den Sicherungsjob vergeben werden.

Name:

Sicherung

- Es kann eine Beschreibung hinzugefügt werden.

Beschreibung:

Sicherung von Daten

- Das Sicherungsziel muss zugewiesen werden. (Hier können nur die vorher dem Agent zugewiesenen Vault Profile ausgewählt werden.)

Ziel:

Vault-Profil

- Hier wird die Art der Protokollierung des Jobs festgelegt. Im normalen Betrieb sollte „**Summary**“ vollkommen ausreichen.

Optionen für Protokolldatei:

Summary

- Hier kann die Verschlüsselungsart ausgewählt werden. Standardmäßig ist „**AES**“ ausgewählt. Sollten Sie bei der Installation des Agents eine eigene Verschlüsselungsbibliothek installiert haben,

Verschlüsselungseinstellungen:

AES (256 Bit)

steht Ihnen diese hier ebenfalls zur Verfügung. Alternativ wird auch die Möglichkeit geboten die Verschlüsselung abzuschalten. Allerdings nehmen die Sicherungsserver der microPLAN GmbH unverschlüsselte Sicherungen nicht an.

6. Abschließend wird noch das Verschlüsselungskennwort vergeben.

Kennwort:

Kennwort bestätigen:

Kennwort-Hinweis:

Hinweis zum Verschlüsseln:

1. Bewahren Sie das Verschlüsselungskennwort gut auf. Ohne das Verschlüsselungskennwort ist kein Zugriff auf Ihre gesicherten Daten und somit auch keine Wiederherstellung möglich.

2. Wenn das Verschlüsselungskennwort geändert wird, wird automatisch eine neue Vollsicherung durchgeführt.

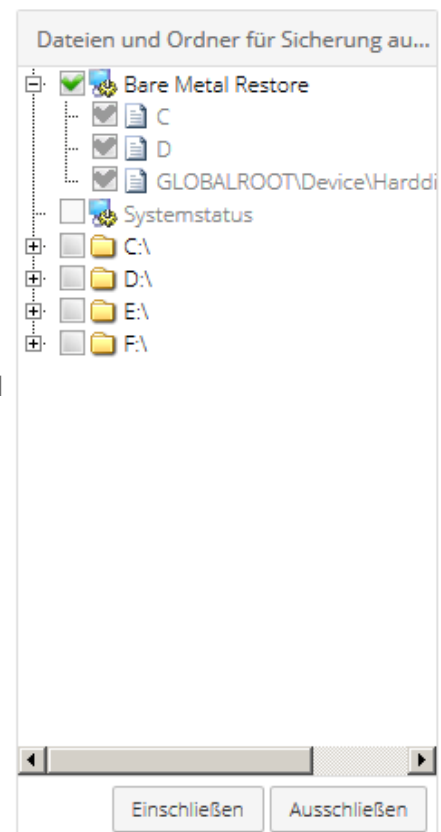
Für eine BMR-Sicherung muss nun in der mittleren Spalte mindestens der Punkt **„Bare Metal Restore“** ausgewählt werden. Dieser umfasst alles was zur Wiederherstellung eines startfähigen Systems nötig ist; also alle Partitionen auf denen Systemkomponenten installiert sind.

Achtung:

1. Laufwerke die keine systemrelevanten Installationen enthalten, werden bei der Auswahl nicht berücksichtigt und müssen separat ausgewählt werden. Im Beispiel rechts werden durch die Auswahl des **„Bare Metal Restore“** nur die Partitionen C:\ und D:\ gesichert. E:\ und F:\ werden nicht gesichert.

2. Wenn Sie in einer BMR-Sicherung Ausschlüsse vorgenommen werden, ist äußerste Vorsicht geboten:

Der Agent prüft nicht ob die Ausschlüsse die Startfähigkeit eines wiederhergestellten Systems beeinträchtigen. Zum Beispiel wäre es ohne Probleme möglich, C:\Windows aus der Sicherung auszuschließen.



Sicherungssatz		
Ordnerfilter	Dateifilter	Rekursiv
+ Bare Metal Res... 		

Für den „**Bare Metal Restore**“ können keine Dateien oder Ordnerfilter erstellt werden.

Nachdem Sie die Auswahl fertig gestellt haben, speichern Sie den Job mit „**Job erstellen**“.

- Nachdem Sie den Job erstellt haben, haben Sie nun noch die Möglichkeit einen Zeitplan für die Ausführung des Jobs zu erstellen.

Zeitplan anzeigen/hinzufügen

vagent-Test, TEST02

Zeitplan hinzufügen

Aufbewahrung	Zeitplan	Komprimierung	Wird zurückgestellt (0 für keine)	Aktivieren	Priorität
Daily	11:30 PM Mo,Tu,We,Th,Fr	Better	0 None	☒	▲ ▼

Speichern
Abbrechen

Anlegen eines Zeitplans im Detail

Aufbewahrung

Hier müssen Sie einen „Aufbewahrungstyp“ auswählen, der das Aufbewahrungsmuster Ihrer Sicherung bestimmt.

Zeitplan

Hier stellen Sie ein, wann und wie spät Ihre Sicherung ausgeführt wird. Zur Auswahl stehen Tage der Woche, Tage des Monats sowie die Möglichkeit eigene Startzeitpunkte zu definieren.

Achtung: Beachten Sie das US Zeitformat AM / PM.

Komprimierung

Hier kann der Grad der Komprimierung eingestellt werden. Den besten Kompromiss zwischen Rechenlast und Komprimierungsgrad bietet „**Better**“.

Wird zurückgestellt

Diese Option bietet die Möglichkeit nach einem bestimmten Zeitfenster die Sicherung abubrechen und die noch

	nicht gesicherten Daten bis zur nächsten Sicherung zurückzustellen. Achtung: Da bei der nächsten Sicherung die Prüfung der Dateien auf Änderungen von vorne beginnt, kann dies dazu führen, dass wenn die Menge der geänderten Daten dauerhaft zu groß für das Sicherungszeitfenster ist, Daten am Ende der Auswahl nie gesichert werden.
Aktivieren	Diese Option aktiviert und deaktiviert den Zeitplan.
Priorität	In Zeitplänen mit mehreren einzelnen Zeitplänen können diese über die Prioritätspfeile sortiert werden. Achtung: Bei mehreren Zeitplänen wird immer der erste zutreffende verwendet.

1. Vom System wird bei der Konfiguration automatisch ein Zeitplan angelegt. Weitere Zeitpläne können Sie oben rechts über den Button „**+Zeitplan Hinzufügen**“ hinzufügen. Hierbei ist zu beachten, dass der Zeitplan der am seltensten ausgeführt wird, an oberster Stelle steht.

Möchten Sie also eine Sicherung erstellen die täglich läuft und zusätzlich eine Wochen- und Monatssicherung durchführt, müsste als oberstes die Monatssicherung aufgeführt werden, dann die Wochensicherung und als unterstes die Tagessicherung. Wenn mehrere Zeitpläne gleichzeitig zutreffen, aber die Sicherung nur einmal durchgeführt werden soll (zum Beispiel bei einer Tagessicherung, die jeden Tag läuft und einer Monatssicherung die an jedem ersten des Monats ausgeführt wird), muss der Startzeitpunkt gleich sein.

Sobald alle Einstellungen getroffen wurden beenden Sie die Konfiguration des Jobs, indem Sie auf „**Speichern**“ klicken.

4.3. Einrichtung einer Sicherung eines UNC-Dateien

1. Um eine Sicherung von Dateien eines UNC-Pfades anzulegen, wählen Sie den Menüpunkt „**Neuen Job für UNC-Dateien erstellen**“.
2. Nachdem Sie „**Neuen Job für UNC-Dateien erstellen**“ gewählt haben, werden im ersten Schritt die Zugangsdaten des UNC-Pfades abgefragt. Hier müssen der vollständige Pfad der Freigabe sowie Zugangsdaten eines Benutzers und der Vollzugriff auf alle zu sichernden Daten die der Pfad besitzt, angegeben werden.

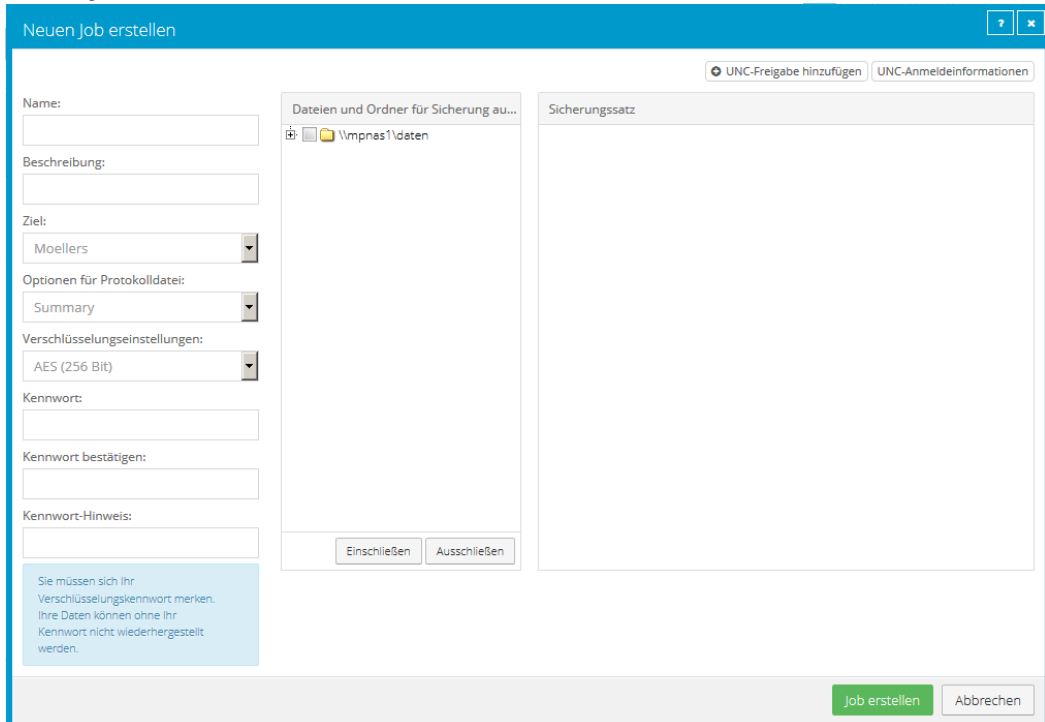


The dialog box titled 'Mit UNC-Freigabe verbinden' contains the following fields:

- Pfad zur Netzwerk-UNC-Freigabe:** \has1\daten (with a note: (z. B. \\192.168.1.1\SomeShare))
- Benutzername:** User
- Kennwort:** (masked with dots)
- Domäne:** domain.local

Buttons: OK, Abbrechen

3. Nachdem Sie die Zugangsdaten übergeben haben, öffnet sich das Fenster für einen neuen Job.



The 'Neuen Job erstellen' window has the following sections:

- Name:** (empty text field)
- Beschreibung:** (empty text field)
- Ziel:** Moellers (dropdown menu)
- Optionen für Protokolldatei:** Summary (dropdown menu)
- Verschlüsselungseinstellungen:** AES (256 Bit) (dropdown menu)
- Kennwort:** (empty text field)
- Kennwort bestätigen:** (empty text field)
- Kennwort-Hinweis:** (empty text field)
- Files and folders for backup:** \mpnas1\daten (tree view)
- Backup settings:** (empty text area)

Buttons: UNC-Freigabe hinzufügen, UNC-Anmeldeinformationen, Einschießen, Ausschießen, Job erstellen, Abbrechen

Warning message: Sie müssen sich Ihr Verschlüsselungskennwort merken. Ihre Daten können ohne Ihr Kennwort nicht wiederhergestellt werden.

Neuen Job erstellen im Detail – Part 1 von 2

Um einen neuen Job zu erstellen, müssen in der linken Spalte folgende Einstellungen als erstes vorgenommen werden:

1. Es muss ein Name für den Sicherungsjob vergeben werden.

Name:

Sicherung

2. Es kann eine Beschreibung hinzugefügt werden.

Beschreibung:

Sicherung von Daten

3. Das Sicherungsziel muss zugewiesen werden. (Hier können nur die vorher dem Agent zugewiesenen Vault Profile ausgewählt werden.)

Ziel:

Vault-Profil

4. Hier wird die Art der Protokollierung des Jobs festgelegt. Im normalen Betrieb sollte „**Summary**“ vollkommen ausreichen.

Optionen für Protokolldatei:

Summary

5. Hier kann die Verschlüsselungsart ausgewählt werden. Standardmäßig ist „**AES**“ ausgewählt. Sollten Sie bei der Installation des Agents eine eigene Verschlüsselungsbibliothek installiert haben, steht Ihnen diese hier ebenfalls zur Verfügung. Alternativ wird hier auch die Möglichkeit geboten die Verschlüsselung abzuschalten. Allerdings nehmen die Sicherungsserver der microPLAN GmbH unverschlüsselte Sicherungen nicht an.

Verschlüsselungseinstellungen:

AES (256 Bit)

6. Abschließend wird noch das Verschlüsselungskennwort vergeben.

Kennwort:

Hinweis zum Verschlüsseln:

1. Bewahren Sie das Verschlüsselungskennwort gut auf. Ohne das Verschlüsselungskennwort ist kein Zugriff auf Ihre gesicherten Daten und somit auch keine Wiederherstellung möglich.

Kennwort bestätigen:

Kennwort-Hinweis:

2. Wenn das Verschlüsselungskennwort geändert wird, wird automatisch eine neue Vollsicherung durchgeführt.

Neuen Job erstellen im Detail – Part 2 von 2

Nun können Sie in der mittleren Spalte festlegen was gesichert werden soll. Sobald ausgewählt ist was gesichert werden soll, ist diese mit „**Einschließen**“ zu bestätigen. Über „**Ausschließen**“ können bestimmte Unterordner ausgeschlossen werden.

Dateien und Ordner für Sicherung au...



 \\mpnas1\daten

Sicherungssatz

	Ordnerfilter	Dateifilter	Rekursiv	
+ daten	z. B. a*, b*	*.*	☒	x trash

Abschließend haben Sie in der rechten Spalte noch die Möglichkeit, über den „**Filter**“ Ordner mit bestimmten Namen oder Namensteilen sowie bestimmte Dateien aus der Auswahl auszuschließen. Hierbei ist zu beachten, dass nur der Dateifilter rekursiv angewendet werden kann. Ein Ordnerfilter gilt immer nur für die oberste Ordnebene der Auswahl.

Nachdem Sie die Auswahl der zu sichernden Daten fertig gestellt haben, speichern Sie den Job mit „**Job erstellen**“.

- Nachdem Sie den Job erstellt haben, haben Sie nun noch die Möglichkeit einen Zeitplan für die Ausführung des Jobs zu erstellen.

Zeitplan anzeigen/hinzufügen

vagent-Test, TEST02

Aufbewahrung	Zeitplan	Komprimierung	Wird zurückgestellt (0 für keine)	Aktivieren	Priorität
Daily	11:30 PM Mo,Tu,We,Th,Fr	Better	0 None	☒	up down trash

Anlegen eines Zeitplans im Detail - Part 1 von 2

Aufbewahrung Hier müssen Sie einen Aufbewahrungstyp auswählen, der das Aufbewahrungsmuster Ihrer Sicherung bestimmt.

Zeitplan Hier stellen Sie ein, wann und wie spät Ihre Sicherung ausgeführt wird. Zur Auswahl stehen Tage der Woche, Tage des Monats sowie die Möglichkeit eigene Startzeitpunkte zu definieren.

Achtung: Beachten Sie das US Zeitformat AM / PM.

Komprimierung Hier kann der Grad der Komprimierung eingestellt werden. Den besten Kompromiss zwischen Rechenlast und Komprimierungsgrad bietet „**Better**“.

Anlegen eines Zeitplans im Detail - Part 2 von 2

Wird zurückgestellt Diese Option bietet die Möglichkeit nach einem bestimmten Zeitfenster die Sicherung abzuberechnen und die noch nicht gesicherten Daten bis zur nächsten Sicherung zurückzustellen.
Achtung: Da bei der nächsten Sicherung die Prüfung der Dateien auf Änderungen von vorne beginnt, kann dies dazu führen, dass wenn die Menge der geänderten Daten dauerhaft zu groß für das Sicherungszeitfenster ist, Daten am Ende der Auswahl nie gesichert werden.

Aktivieren Diese Option aktiviert und deaktiviert den Zeitplan.

Priorität In Zeitplänen mit mehreren einzelnen Zeitplänen können diese über die Prioritätspfeile sortiert werden.

Achtung: Bei mehreren Zeitplänen wird immer der erste zutreffende verwendet.

- Vom System wird bei der Konfiguration automatisch ein Zeitplan angelegt. Weitere Zeitpläne können Sie oben rechts über den Button „**+Zeitplan Hinzufügen**“ hinzufügen. Hierbei ist zu beachten, dass der Zeitplan der am seltensten ausgeführt wird an oberster Stelle steht.

Möchten Sie also eine Sicherung erstellen, die täglich läuft und zusätzlich eine Wochen- und Monatssicherung durchführt, müsste als oberstes die Monatssicherung aufgeführt werden, dann die Wochensicherung und als unterstes die Tagessicherung. Wenn mehrere Zeitpläne gleichzeitig zutreffen können, aber die Sicherung nur einmal durchgeführt werden soll (zum Beispiel bei einer Tagessicherung, die jeden Tag läuft und einer Monatssicherung, die an jedem ersten des Monats ausgeführt wird), muss der Startzeitpunkt gleich sein.

Sobald alle Einstellungen getroffen wurden, beenden Sie die Konfiguration des Jobs, indem Sie auf „**Speichern**“ klicken.

Hinweise: Bei dieser Art der Sicherung wird kein VSS verwendet. Daher können Dateien, die sich im Zugriff befinden, nicht gesichert werden.

Es wird empfohlen pro Sicherungsjob nur einen UNC-Pfad zu sichern, also für jeden UNC-Pfad einen eigenen Job anzulegen.

4.4. Änderung von bestehenden Sicherungen

Wenn Sie Änderungen an einer bestehenden Sicherung vornehmen möchten, gehen Sie wie folgt vor:

1. Klicken Sie in der Navigation auf den Menüpunkt „**Computer**“.

Dashboard Computer Überwachung Berichte Richtlinien

2. Wählen Sie den Computer an dem Sie Änderungen vornehmen wollen.

Computer ▲		Gruppen
☐		Alle ▼
☐	 MP	

3. Es öffnet sich nun die Übersicht mit allen „**Jobs**“, die zu diesem Computer vorhanden sind.

Name	Jobtyp	Beschreibung	Letzter Sicherungsstatus	Letzte Ausführung	Aktion
Tagessicherung	Lokales System	Sicherung	✓ Abgeschlossen	yesterday at 21:10	Aktion auswählen ▼

4. Unter „**Aktion**“ haben Sie die Möglichkeit die gewünschte Aktion zu wählen.

Aktion im Detail

Um eine Aktion zum Job zu hinterlegen ist es nötig auf „**Aktion auswählen**“ zu klicken.

1. Job bearbeiten
2. Zeitplan anzeigen/hinzufügen
3. Job ausführen
4. Wiederherstellen
5. Synchronisieren
6. Verlauf/Protokolle
7. Job löschen

Aktion auswählen ▼
Job bearbeiten
Zeitplan anzeigen/hinzufügen
Job ausführen
Wiederherstellen
Synchronisieren
Verlauf/Protokolle
Job löschen

5. Restore von Datensicherungen

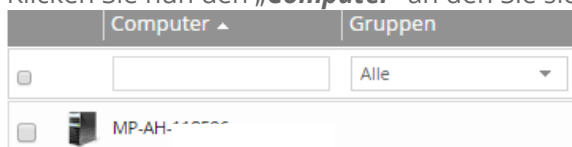
Im Fall des Falles ist es nötig Daten aus einer Datensicherung wiederherzustellen. Damit Daten wiederhergestellt werden können, gehen Sie bitte wie folgt vor.

5.1. Restore einer filebasierenden Datensicherung

1. Klicken Sie in der Navigation auf den Menüpunkt „**Computer**“.

Dashboard **Computer** Überwachung Berichte Richtlinien

2. Klicken Sie nun den „**Computer**“ an den Sie sichern möchten.



3. Wählen Sie nun den Menüpunkt „**Jobs**“.

Jobs Vault-Einstellungen Erweitert

4. Es öffnet sich nun die Übersicht mit allen „**Jobs**“, die zu diesem Computer vorhanden sind.

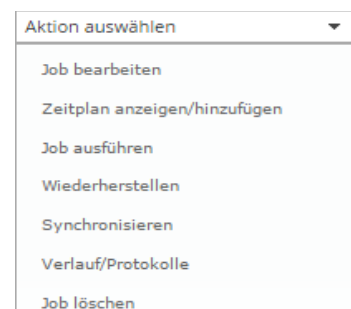
Name	Jobtyp	Beschreibung	Letzter Sicherungsstatus	Letzte Ausführung	Aktion
Tagessicherung	Lokales System	Sicherung	✓ Abgeschlossen	yesterday at 21:10	Aktion auswählen

5. Wählen Sie nun unter „**Aktion auswählen**“ den Punkt „**Wiederherstellen**“.

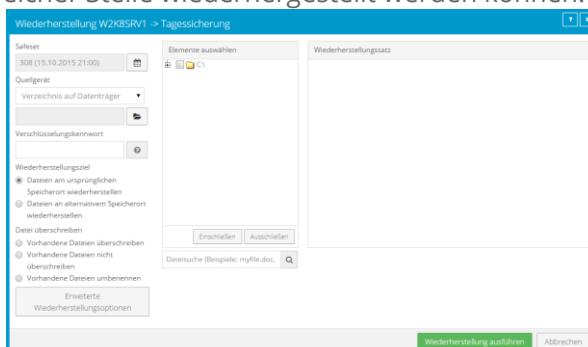
Aktion im Detail

Um eine Aktion zum Job zu hinterlegen ist es nötig auf „**Aktion auswählen**“ zu klicken.

1. Job bearbeiten
2. Zeitplan anzeigen/hinzufügen
3. Job ausführen
4. Wiederherstellen
5. Synchronisieren
6. Verlauf/Protokolle
7. Job löschen



Es öffnet sich nun das Fenster mit dessen Hilfe Sie wählen können, welche Daten an welcher Stelle wiederhergestellt werden können.



Wiederherstellen im Detail – Part 1 von 2

Safeset:

Hier legen Sie fest von welchem Zeitpunkt Sie die Daten wiederherstellen möchten. Automatisch wird immer das neuste Backup vorgeschlagen.

Safeset

308 (15.10.2015 21:00)



Quellgerät:

Als nächstes wählen Sie aus, von wo Sie wiederherstellen wollen. Im Normalfall ist dies immer Ihr Vault Profil.

Quellgerät

Verzeichnis auf Datenträger



Wenn sehr große Datenmengen wiederhergestellt werden müssen, ist es aber auch möglich diese auf einen Datenträger exportieren zu lassen, der Ihnen dann zugesandt wird und dann bei der Wiederherstellung als Quelle dient. Bei dem Export handelt es sich weiterhin um verschlüsselte Dateien, die bei der Wiederherstellung entschlüsselt werden.

Verschlüsselungskennwort:

Hier müssen Sie das Verschlüsselungskennwort, das Sie bei der Einrichtung der Sicherung vergeben haben, eingeben.

Verschlüsselungskennwort



Hinweis: Ohne das Kennwort ist keine Wiederherstellung möglich.

Wiederherstellungsziel:

Hier wird festgelegt wo auf dem Server die Daten wiederhergestellt werden sollen. Standardmäßig ist der ursprüngliche Speicherort ausgewählt. Es kann aber auch ein neues Ziel vorgegeben werden. Dieses muss aber vorher auf dem System angelegt worden sein.

Wiederherstellungsziel

- ☒ Dateien am ursprünglichen Speicherort wiederherstellen
- ☐ Dateien an alternativem Speicherort wiederherstellen

Wiederherstellen im Detail – Part 2 von 2

Datei überschreiben

Hier muss festgelegt werden wie mit im Wiederherstellungsziel vorhandenen Dateien verfahren werden soll.

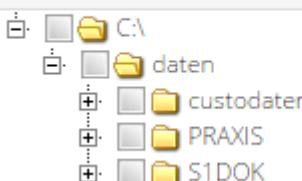
Datei überschreiben

- ☐ Vorhandene Dateien überschreiben
- ☐ Vorhandene Dateien nicht überschreiben
- ☐ Vorhandene Dateien umbenennen

Erweiterte
Wiederherstellungsoptionen

In der mittleren Spalte kann nun ausgewählt werden, welche Daten wiederhergestellt werden sollen. Anschließend bestätigen Sie die Auswahl mit „**Einschließen**“. Sollen bestimmte Unterordner oder Dateien eines ausgewählten Ordners nicht mit wiederhergestellt werden, können diese über „**Ausschließen**“ ausgeschlossen werden.

Elemente auswählen



Dateisuche (Beispiele: myfile.doc, )

Wiederherstellungssatz

	Ordnerfilter	Dateifilter	Rekursiv	
 daten	z. B. a*, b*	*. *	☒	 

Wiederherstellungssatz muss angewendet werden, bevor Wiederherstellung durchgeführt

Nachdem Sie Ihre wiederherzustellenden Daten gewählt haben, haben Sie in der rechten Spalte die Möglichkeit Filter für Ordner oder Daten zu definieren, die nicht mit wiederhergestellt werden sollen. Haben Sie einen Filter definiert, müssen Sie diesen mit „**Jetzt anwenden**“ bestätigen.

Zum Schluss müssen Sie auf „**Wiederherstellungen ausführen**“ klicken. Somit wird die Wiederherstellung ausgeführt.

5.2. Restore einer BMR-Sicherung

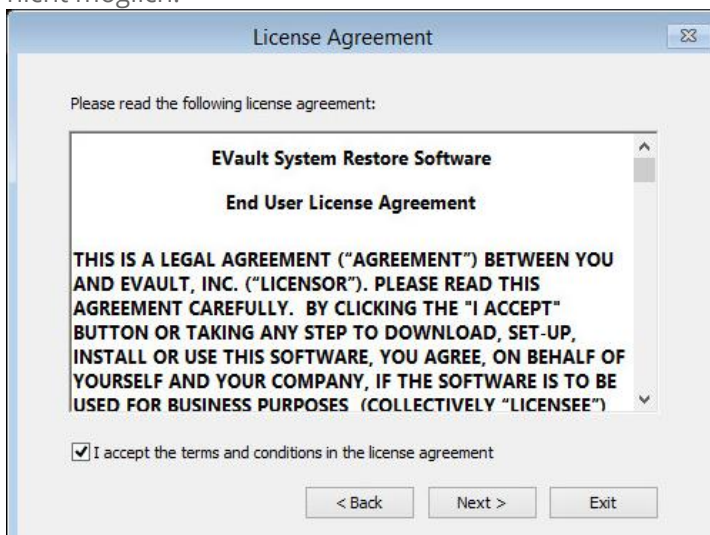
Zum Wiederherstellen einer BMR-Sicherung ist ein Wiederherstellungsmedium notwendig.

Dieses sollte für Ihr Zielsystem individuell erstellt werden, da Sie so die Möglichkeit haben die für Ihr Zielsystem nötigen Treiber einzubinden. Genauere Informationen hierzu finden Sie in der Anleitung „**EVault BMR Medium erstellen**“ im Downloadbereich.

1. Legen Sie Ihre Boot CD ein und starten Sie von der CD. Stellen Sie die gewünschte Sprache und das Tastaturlayout ein. Klicken Sie nun auf „**Next**“



2. Bestätigen Sie die Lizenzbedingungen! Ohne Bestätigung ist die Wederherstellung nicht möglich!



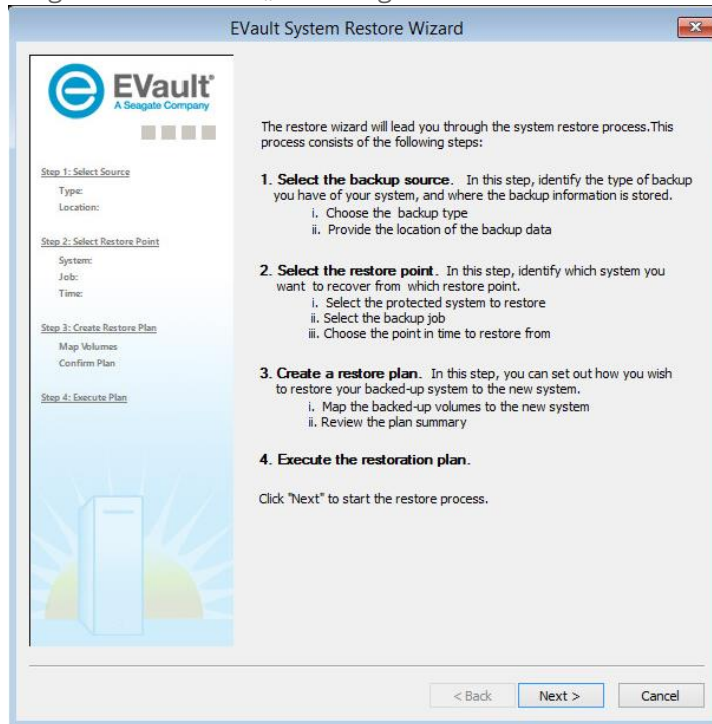
3. Sie gelangen nun zum „**EVault System Restore Main Menu**“
Sie haben nun die Möglichkeit eine der folgenden 4 Optionen zu wählen:



EVault System Restore Main Menu im Detail

Restore My System	Diese Option bietet Ihnen die Möglichkeit den Restore Prozess zu starten. Sie werden hier Schritt für Schritt durch ein Menu geleitet.
Repair My System	Hier haben Sie die Möglichkeit nötige Treiber für den Start nach einer Wiederherstellung auszutauschen.
Restore Test Run	Mit dieser Option haben Sie die Möglichkeit einen Wiederherstellungstest durchzuführen. Es werden dabei keine Änderungen am System vorgenommen.
Settings	Diese Option bietet Ihnen die Möglichkeit Netzwerkeinstellungen zu ändern oder anzupassen, IP-Adressen zu vergeben oder Treiber des gebooteten Images zu aktualisieren. Weitere Optionen sind: Disk Settings und Log Settings.

4. Um eine Wiederherstellung mit BMR durchzuführen, wählen Sie die Option 1. **„Restore My System“**. Sie werden nun auf den Ablauf des Restore Prozesses hingewiesen. Dieser „Wizard“ geht mit Ihnen Schritt für Schritt vor.



EVault System Restore Wizard im Detail

Select the Backup source	Wählen Sie die Wiederherstellungsquelle. Diese kann der Backup Satellit der Vault oder eine lokale Festplatte sein.
Select the restore point	Je nachdem wie viele BMR-Sicherungen Sie bereits gefahren haben, stehen Ihnen hier verschieden Sicherungen zur Verfügung.
Create a restore plan	Zeigt Ihnen die Zusammenfassung Ihrer gesetzten Einstellungen.
Execute the restoration plan	Führt die Wiederherstellung aus.

5. Nachdem Sie den Wizard mit „**Next**“ gestartet haben, müssen Sie die Wiederherstellungsquelle auswählen.

Choose Backup Location im Detail

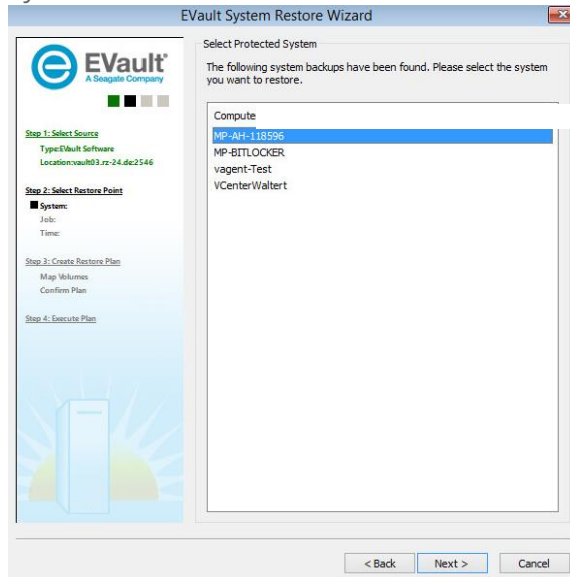
Vault IP	Name oder IP des Vault oder Satelliten, z.B. Vault03.rz-24.de.
Account	Entspricht dem „ Konto “ unter den Vault-Einstellungen.
Username	Entspricht dem „ Benutzernamen “ unter den Vault-Einstellungen.
Password	Das Kennwort erhalten Sie auf Anfrage bei unserer EVault Abteilung. Achtung: Das ist nicht das Kennwort der Verschlüsselung!
Advanced Settings	Hier können Einstellungen zum Port und der Wiederverbindungszeit getroffen werden.

Hinweis: Die benötigten Informationen können Sie bei Bedarf über das Web Frontend unter den Vault-Einstellungen finden. Dabei ist zu bedenken, dass die Kennwörter hier nicht angezeigt werden! Diese finden Sie unter:

Computer / „Gesicherter Rechner“ / Vault-Einstellungen / Aktion „Bearbeiten“

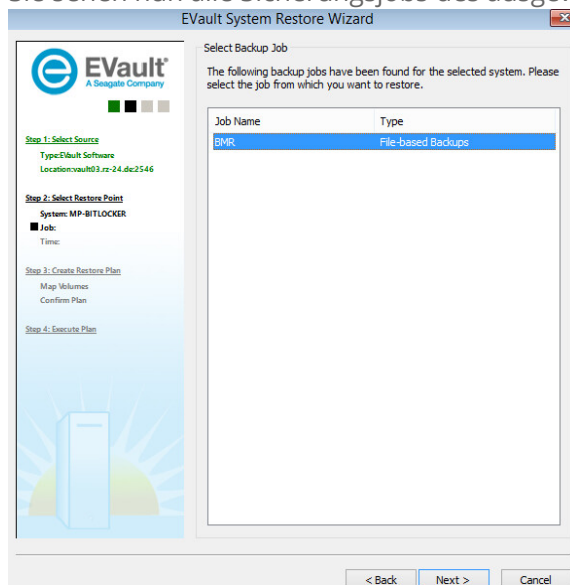
Ein weiterer wichtiger Punkt ist „**Restore Settings**“. Hier haben Sie die Möglichkeit eventuell fehlende Netzwerktreiber nachzuladen.

6. Sobald Sie Ihre Zugangsdaten eingegeben haben, können Sie auf „**Next**“ klicken. Sie bekommen hier nun eine Auswahl der unter diesem Vault Konto gesicherten Systemen.



Wählen Sie den entsprechend wiederherzustellenden Rechner aus und fahren Sie mit „**Next**“ fort.

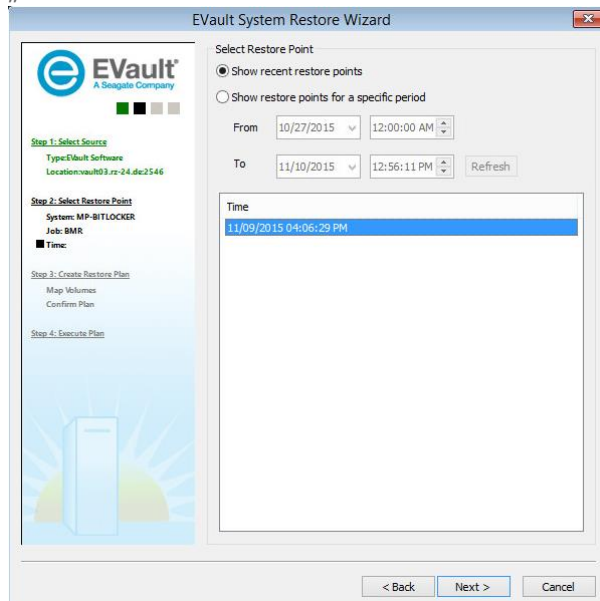
7. Sie sehen nun alle Sicherungsjobs des ausgewählten Systems.



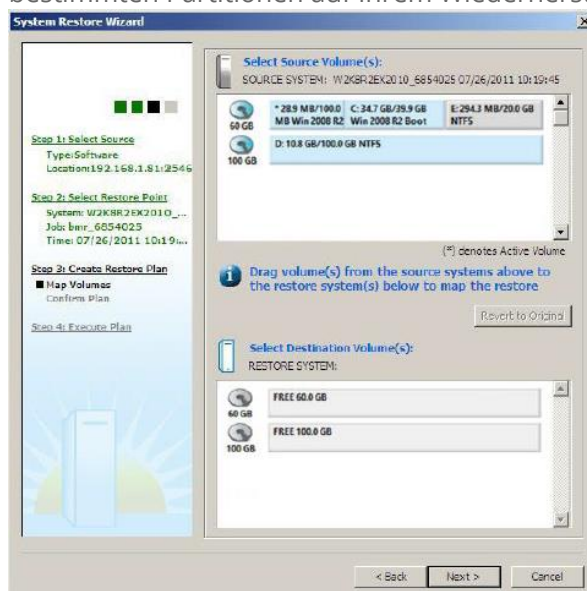
Bitte bedenken Sie, dass **nur** BMR-Sicherungen über das Wiederherstellungsmedium wiederhergestellt werden können. Prüfen Sie daher, welche Sicherung eine „**BMR**-Sicherung“ war. Dieses können Sie -falls nicht mehr bekannt- im Web Frontend prüfen.

Wählen Sie den entsprechenden Job aus und fahren Sie mit „**Next**“ fort.

8. Im nächsten Schritt wählen Sie aus, welche Sicherung Sie wiederherstellen wollen. Sie haben hier die Möglichkeit einen Filter zu setzen, sodass nur Sicherungen aus einem bestimmten Zeitraum angezeigt werden. Bestätigen Sie anschließend mit „Next“.



9. Nun können Sie via „**Drag and Drop**“ die in der Sicherung enthaltenen Partitionen zu bestimmten Partitionen auf Ihrem Wiederherstellungsziel zuordnen.



Achtung: Sie haben nun die Möglichkeit die Ziel HDD so anzupassen, dass Sie auch MBR-Sicherung auf ein UEFI-System installieren können. Klicken Sie dazu mit der rechten Maustaste auf die Ziel HDD. Sie haben nun die Möglichkeit die HDD in „**GPT disk**“ oder „**MBR disk**“ zu konvertieren. Grundsätzlich bekommen Sie beim Drag und Drop eine entsprechende Information.

10. In den folgenden Fenstern bekommen Sie eine Zusammenfassung der geplanten Wiederherstellung angezeigt. Sollte diese für Sie in Ordnung sein, so müssen Sie **„Click here to confirm the restore plan“** auswählen, bevor Sie auf **„Next“** klicken.
11. Nun startet die Wiederherstellung. Je nach Größe der Sicherung und der zur Verfügung stehenden Bandbreite zur Wiederherstellungsquelle, kann dieses einige Zeit in Anspruch nehmen.
12. Nach Abschluss der Wiederherstellung haben Sie die Möglichkeit Treiber für die neue Hardware auszutauschen. Dieses sollte entsprechend auch gemacht werden. Wichtig sind z. B. die Treiber für den HDD Controller.
13. Nun muss das System abschließend neugestartet werden. Nach dem Neustart ist es nötig, fehlende Treiber unter Windows zu installieren.